CHAPTER 10

Alarm Monitoring and Management

This chapter explains how to manage alarms with Cisco Transport Controller (CTC), which includes:

To troubleshoot specific alarms, refer to the *Cisco ONS 15600 Troubleshooting Guide*.

10.1 Overview

CTC detects and reports SONET alarms generated by the Cisco ONS 15600 and the larger SONET network. You can use CTC to monitor and manage alarms at the card, node, or network level. Default alarm severities conform to the Telcordia GR-253 standard, but you can set alarm severities in customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by Optical Networking System (ONS) nodes, refer to the *Cisco ONS 15600 Troubleshooting Guide.*

Note ONS 15600 alarms can also be monitored and managed through TL1 or a network management system (NMS).

10.2 Alarms, Conditions, and History

In the card, node, or network level CTC view, click the Alarms tab to display the alarms for that card, node or network. The Alarms window shows alarms in conformance to Telcordia GR-253. This means that if a network problem causes two alarms, such as loss of frame (LOF) and loss of signal (LOS), CTC only shows the LOS alarm in this window because it supersedes the LOF.

Table 10-1 describes in the information in the Alarms window.

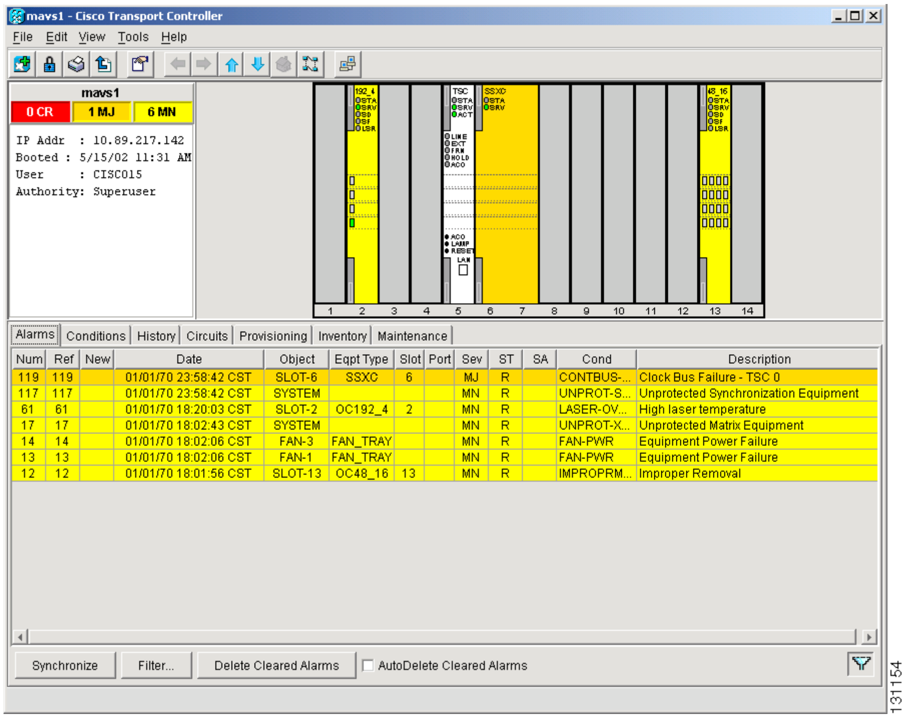
Table 10-1 Alarms Column Descriptions

Column	Information Recorded
Num	Quantity of alarm messages received; incremented automatically as alarms occur to display the current total of received error messages
Ref	A unique identification number assigned to each alarm to reference a specific alarm message that is displayed
New	Indicates a new alarm if checked[1]
Date	Date and time of the alarm
Object	TL1 access identifier (AID) for the alarmed object
Eqpt Type	Card type in this slot
Slot	Slot where the alarm occurred (appears in the network view and node view)
Port	Port where the alarm occurred
Sev	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR)
ST	Status: Raised (R), Clear (C), Transient (T)
SA	When checked, indicates a service-affecting alarm
Cond	Error message/alarm name; alphabetically defined in the *Cisco ONS 15600 Troubleshooting Guide*
Description	Description of the alarm
Node	Node where the alarm occurred (only displayed in network view)

[1] The user can click the Synchronize button to acknowledge the new alarm. Clicking the Delete Cleared Alarms button only deletes cleared alarms on the window.

Figure 10-1 shows the CTC node view Alarms window.

Figure 10-1 Viewing Alarms in CTC Node View


mavs1 - Cisco Transport Controller
File Edit View Tools Help
mavs1
0 CR
1 MJ
6 MN
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Synchronize
Filter...
Delete Cleared Alarms
□ AutoDelete Cleared Alarms
131154

```
IP Addr  : 10.89.217.142
Booted : 5/15/02 11:31 AM
User     : CISC015
Authority: Superuser
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
119	119		01/01/70 23:58:42 CST	SLOT-6	SSXC	6		MJ	R		CONTBUS-...	Clock Bus Failure - TSC 0
117	117		01/01/70 23:58:42 CST	SYSTEM				MN	R		UNPROT-S...	Unprotected Synchronization Equipment
61	61		01/01/70 18:20:03 CST	SLOT-2	OC192_4	2		MN	R		LASER-OV...	High laser temperature
17	17		01/01/70 18:02:43 CST	SYSTEM				MN	R		UNPROT-X...	Unprotected Matrix Equipment
14	14		01/01/70 18:02:06 CST	FAN-3	FAN_TRAY			MN	R		FAN-PWR	Equipment Power Failure
13	13		01/01/70 18:02:06 CST	FAN-1	FAN_TRAY			MN	R		FAN-PWR	Equipment Power Failure
12	12		01/01/70 18:01:56 CST	SLOT-13	OC48_16	13		MN	R		IMPROPRM...	Improper Removal

Alarms and conditions appear in one of five background colors, listed in Table 10-2, to communicate severity.

Table 10-2 Color Codes for Alarms and Conditions

Color	Description
Red	Critical alarm
Orange	Major alarm
Yellow	Minor alarm
Magenta (pink)	Event (NA)
Blue	Condition (NR)
White	Cleared alarm or event (C)

Note Major and Minor alarms may appear yellow in CTC under certain circumstances. This is not due to a CTC problem but to a workstation memory and color utilization problem. For example, a workstation might run out of colors if many color-intensive applications are running. When using Netscape, you can limit the number of colors used by launching it from the command line with either the -install option or the -ncols 32 option.

Software Release 5.0 has TL1 port-based alarm numbering that identifies an alarmed synchronous transport signal (STS) by its STS on a port rather than the STS on the optical card. The numbering is present in the STS alarm TL1 AID. The numbering scheme is described in Table 10-3.

Table 10-3 TL1 Port-Based Alarm Numbering Scheme

MON Object (Optical)	Syntax and Examples
OC3/12/48/192 STS	Syntax: STS-<Slot>-<Pim>-<Ppm>-<Port>-<STS> Ranges: STS-{1-4,11-14}-{1-4}-{1-4}-{1-n[1]}-{1-n[2]} Example: STS-1-1-1-1-6

[1] Port number range varies by card type with a maximum of four.

[2] Maximum STS number depends on the rate and size of the STS.

10.2.1 Alarm Window

Table 10-4 shows the actions you can perform in the Alarms window.

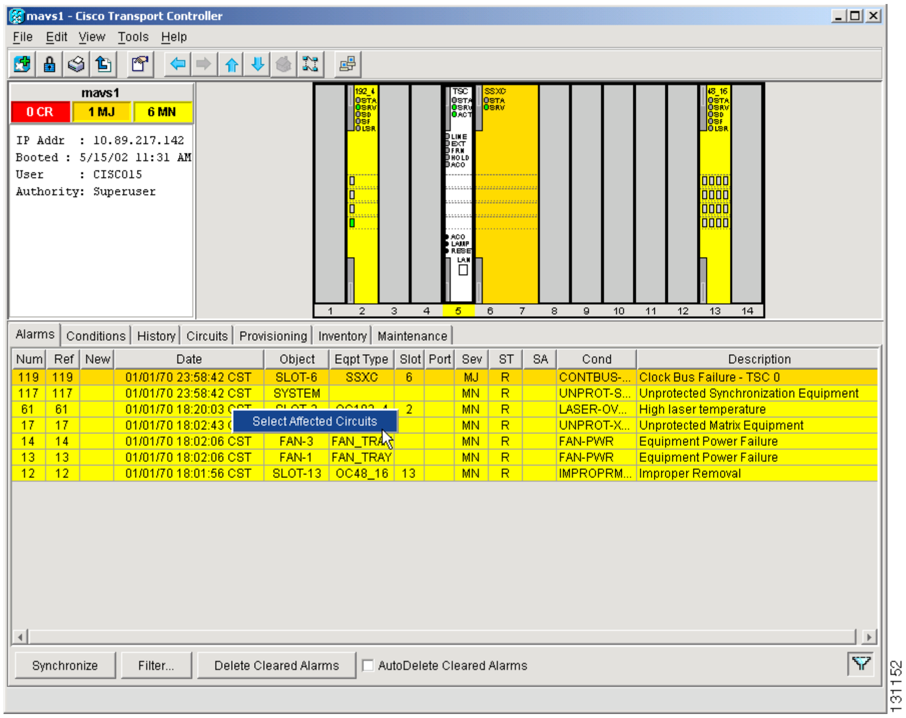
Table 10-4 Alarm Window

Button	Action
Filter	Allows you to change the display on the Alarms window to show only alarms that meet a certain severity level, occur in a specified time frame, and/or reflect specific conditions. For example, you can set the filter so that only critical alarms appear on the window. If you enable the Filter feature by clicking the Filter icon button in one CTC view, such as node view, it is enabled in the others as well (card view and network view).
Synchronize	Updates the alarm display. Although CTC displays alarms in real time, the Synchronize button verifies that CTC and the ONS 15600 agree on current alarms. This is particularly useful during provisioning or troubleshooting.
Delete Cleared Alarms	Deletes alarms that have been cleared.
AutoDelete Cleared Alarms	If checked, CTC automatically deletes cleared alarms.

10.2.2 Alarm-Affected Circuits

You can determine which ONS 15600 circuits are affected by a specific alarm by positioning the cursor over the alarm in the Alarm window and right-clicking. A shortcut menu appears (Figure 10-2).

Figure 10-2 Select the Affected Circuits Option for an Alarm


mavs1 - Cisco Transport Controller
File Edit View Tools Help
192_4
TSC
SSXC
48_16
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Select Affected Circuits
Synchronize
Filter...
Delete Cleared Alarms
131152

mavs1

0 CR | 1 MJ | 6 MN

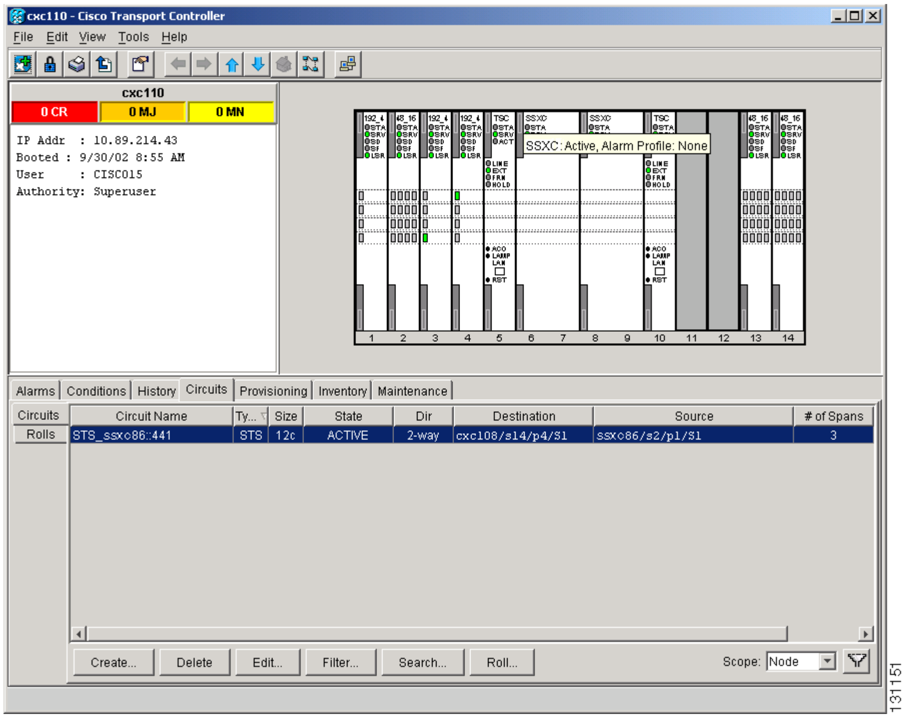
```
IP Addr  : 10.89.217.142
Booted : 5/15/02 11:31 AM
User     : CISCO15
Authority: Superuser
```

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
119	119		01/01/70 23:58:42 CST	SLOT-6	SSXC	6		MJ	R		CONTBUS-...	Clock Bus Failure - TSC 0
117	117		01/01/70 23:58:42 CST	SYSTEM				MN	R		UNPROT-S...	Unprotected Synchronization Equipment
61	61		01/01/70 18:20:03 CST	SLOT-2	OC192_4	2		MN	R		LASER-OV...	High laser temperature
17	17		01/01/70 18:02:43 C					MN	R		UNPROT-X...	Unprotected Matrix Equipment
14	14		01/01/70 18:02:06 CST	FAN-3	FAN_TRA			MN	R		FAN-PWR	Equipment Power Failure
13	13		01/01/70 18:02:06 CST	FAN-1	FAN_TRAY			MN	R		FAN-PWR	Equipment Power Failure
12	12		01/01/70 18:01:56 CST	SLOT-13	OC48_16	13		MN	R		IMPROPRM...	Improper Removal

□ AutoDelete Cleared Alarms

When the user selects the Select Affected Circuits option, the Circuits window opens to show the circuits that are affected by the alarm (Figure 10-3).

Figure 10-3 Alarm-Affected Circuit Appears


cxc110 - Cisco Transport Controller
File Edit View Tools Help
cxc110
0 CR
0 MJ
0 MN
SSXC: Active, Alarm Profile: None
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Alarms Conditions History Circuits Provisioning Inventory Maintenance
Circuits
Rolls
Create... Delete Edit... Filter... Search... Roll...
Scope: Node
131151

```
IP Addr  : 10.89.214.43
Booted : 9/30/02 8:55 AM
User     : CISCO15
Authority: Superuser
```

Circuit Name	Ty...	Size	State	Dir	Destination	Source	# of Spans
STS_ssxc86::441	STS	12c	ACTIVE	2-way	cxc108/s14/p4/S1	ssxc86/s2/p1/S1	3

10.2.3 Conditions Window

The Conditions window displays retrieved fault conditions. A condition is a fault or status detected by ONS 15600 hardware or software. When a condition occurs and continues for a minimum period, CTC raises a condition, which is a flag showing that this particular condition currently exists on the ONS 15600.

The Conditions window shows all conditions that occur, including those that are superseded by alarms. For instance, if a network problem causes two alarms, such as LOF and LOS, CTC shows both the LOF and LOS conditions in this window. Having all conditions visible can be helpful when troubleshooting the ONS 15600. If you want to retrieve conditions that obey a root-cause hierarchy (that is, LOS supersedes and replaces LOF), you can exclude the same root causes.

Fault conditions include reported alarms and Not Reported or Not Alarmed conditions. Refer to the trouble notifications information in the *Cisco ONS 15600 Troubleshooting Guide* for more information about alarm and condition classifications.

10.2.4 Conditions Window Actions

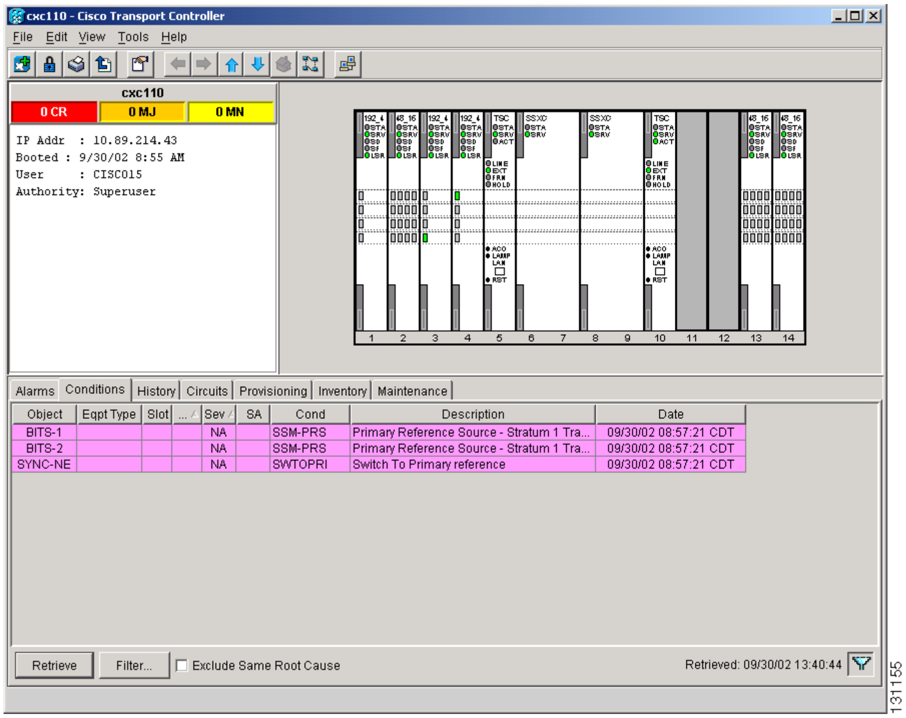
Table 10-5 shows the actions you can perform in the Conditions window.

Table 10-5 Conditions Display

Button	Action
Retrieve	Retrieves the current set of all existing fault conditions, as maintained by the alarm manager, from the ONS 15600.
Filter	Allows you to change the Conditions window display to only show the conditions that meet a certain severity level or occur in a specified time. For example, you can set the filter so that only critical conditions display on the window. There is a Filter icon button in the lower-right corner of the window that allows you to enable or disable the filter feature.

The current set of all existing conditions maintained by the alarm manager appears when you click the Retrieve button. The set of conditions retrieved is relative to the view. For example, if you click the button in the node view, node-specific conditions appear (Figure 10-4). If you click the Retrieve button in the network view, all conditions for the network (including ONS 15600 nodes and other connected nodes such as ONS 15454s) appear, and the card view shows only card-specific conditions.

Figure 10-4 Viewing Conditions in the Conditions Window



IP Addr : 10.89.214.43
Booted : 9/30/02 8:55 AM
User : CISCO15
Authority: Superuser

Object	Eqpt Type	Slot	...	Sev	SA	Cond	Description	Date
BITS-1				NA		SSM-PRS	Primary Reference Source - Stratum 1 Tra...	09/30/02 08:57:21 CDT
BITS-2				NA		SSM-PRS	Primary Reference Source - Stratum 1 Tra...	09/30/02 08:57:21 CDT
SYNC-NE				NA		SWTOPRI	Switch To Primary reference	09/30/02 08:57:21 CDT

☐ Exclude Same Root Cause

Retrieved: 09/30/02 13:40:44

Table 10-6 lists the Conditions window column headings and the information recorded in each column.

Table 10-6 Conditions Column Description

Column	Information Recorded
Date	Date and time of the condition
Object	TL1 AID for the alarmed object
Eqpt Type	Card type in this slot (only displayed in the network view and node view)
Slot	Slot where the condition occurred (only displayed in the network view and node view)
Port	Port where the condition occurred
Sev	Severity level: CR, MJ, MN, NA, NR
SA	When checked, indicates a service-affecting alarm
Cond	Condition name; alphabetically listed and defined in the “Alarm Troubleshooting” chapter of the *Cisco ONS 15600 Troubleshooting Guide*
Description	Description of the condition
Node	Node where the condition occurred (only displayed in network view)

10.2.5 History Window

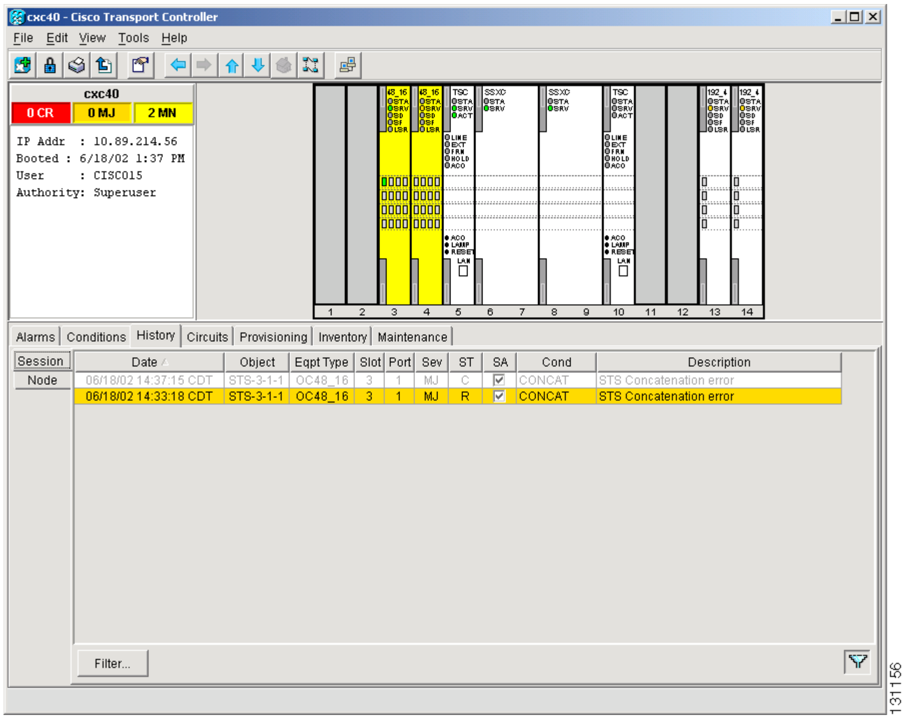
The History window displays historical alarm data. It also displays conditions, which are Not Alarmed activities such as timing changes and threshold crossings. For example, protection-switching events or performance-monitoring threshold crossings appear here. The ONS 15600 can store up to 3,000 total alarms and conditions: 750 critical alarms, 750 major alarms, 750 minor alarms, and 750 conditions. When the limit is reached, the ONS 15600 begins replacing the oldest items. The History window presents several alarm history views:

- The History > Session window appears in network view, node view, and card view (Figure 10-5). It shows alarms and conditions that have occurred during the current user CTC session.
- The History > Node window appears only in node view. It shows the alarms and conditions that have occurred on the node since CTC software was originally activated for that node.
- The History > Card window appears only in the card view. It shows the alarms and conditions that have occurred on the card since CTC software was installed on the node.

Note In the Preference dialog box General tab, the Maximum History Entries value applies to only the Session window.

Tip Double-click an alarm in the History window to display the corresponding view. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Figure 10-5 Viewing All Alarms Reported for Current Session



cxc40 - Cisco Transport Controller

```
IP Addr  : 10.89.214.56
Booted : 6/18/02 1:37 PM
User     : CISCO15
Authority: Superuser
```

Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
06/18/02 14:37:15 CDT	STS-3-1-1	OC48_16	3	1	MJ	C	☑	CONCAT	STS Concatenation error
06/18/02 14:33:18 CDT	STS-3-1-1	OC48_16	3	1	MJ	R	☑	CONCAT	STS Concatenation error

Table 10-7 describes the information in the History window.

Table 10-7 History Column Description

Column	Information Recorded
Num	An incrementing count of alarm or condition messages. (The column is hidden by default; to view it, right-click a column and choose Show Column > Num.)
Ref	The reference number assigned to the alarm or condition. (The column is hidden by default; to view it, right-click a column and choose Show Column > Ref.)
Date	Date and time of the alarm
Object	TL1 AID for the alarmed object
Sev	Severity level: CR, MJ, MN, NA, NR
Eqpt Type	Card type in this slot (only displays in network view and node view)
ST	Status: R, C, T
Description	Description of the condition
Port	Port where the condition occurred
Cond	Condition name
Slot	Slot where the condition occurred (only displays in network view and node view)
SA	When checked, indicates a service-affecting alarm

10.2.6 Alarm History Actions

You can retrieve and view the history of alarms and conditions, as well as transients (passing notifications of processes as they occur) in the CTC History window. The information in this window is specific to the view where it is shown (that is, network history in the network view, node history in the node view, and card history in the card view).

The node and card history views are each divided into two tabs. In node view, when you click the Retrieve button, you can see the history of alarms, conditions, and transients that have occurred on the node in the History > Node window, and the history of alarms, conditions, and transients that have occurred on the node during your login session in the History > Session window. When you retrieve the card history, you can see the history of alarms, conditions, and transients on the card in the History > Card window, or a history of alarms, conditions, and transients that have occurred during your login session in the History > Session window. You can also filter the severities and occurrence period in these history windows.

10.3 Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15600 ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node, cards, or ports.

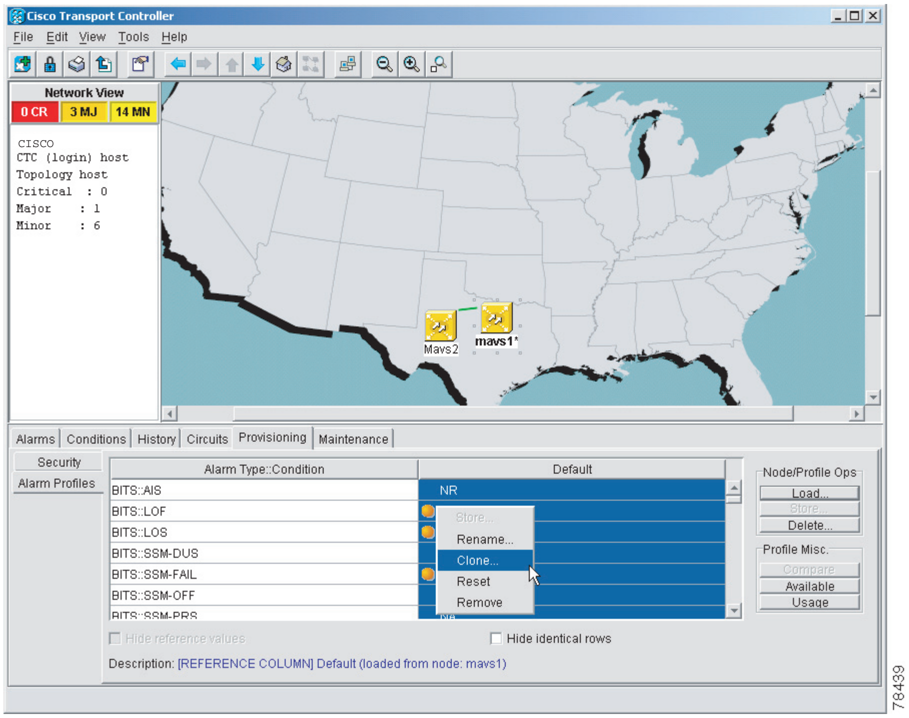
CTC can store up to ten active alarm profiles at any time to apply to the node. Custom profiles can take eight of these active profile positions. Two other profiles, Default profile and Inherited profile, are reserved by the NE, and cannot be edited. The reserved Default profile contains Telcordia GR-253-CORE severities. The reserved Inherited profile allows port alarm severities to be governed by the card-level severities or card alarm severities to be determined by the node-level severities.

If one or more alarm profiles have been stored as files from elsewhere in the network onto the local PC or server hard drive where CTC resides, you can utilize as many profiles as you can physically store by deleting and replacing them locally in CTC so that only eight are active at any given time.

10.3.1 Alarm Profile Window

Alarm profiles are created in the network view using the Provisioning > Alarm Profiles tabs (Figure 10-6). A default alarm profile (in the Default column) is preprovisioned for every alarm. After loading the default profile on the node, you can use the Clone feature to create new profiles based on the default alarm profile. After the new profile is created, the Alarm Profiles window shows the default profile and the new profile.

Figure 10-6 Alarm Profiles Window Showing the Default Profiles of Listed Alarms



```
CISCO
CTC (login) host
Topology host
Critical  : 0
Major     : 1
Minor     : 6
```

Alarm Type::Condition	Default
BITS::AIS	NR
BITS::LOF	
BITS::LOS	
BITS::SSM-DUS	
BITS::SSM-FAIL	
BITS::SSM-OFF	
BITS::SSM-PRS	

□ Hide reference values □ Hide identical rows

Description: [REFERENCE COLUMN] Default (loaded from node: mavs1)

10.3.2 Alarm Profile Buttons

The Alarm Profiles window has six buttons at the bottom. Table 10-8 describes each of the alarm profile buttons.

Table 10-8 Alarm Profile Buttons

Button	Description
New	Adds a new alarm profile.
Load	Loads a profile to a node or a file.
Store	Saves profiles on a node (or nodes) or in a file.
Delete	Deletes profiles from a node.
Compare	Displays differences between alarm profiles (individual alarms that are not configured equivalently between profiles).
Available	Displays all profiles available on each node.
Usage	Displays all entities (nodes and alarm subjects) present in the network and which profiles contain the alarm (can be printed).

10.3.3 Alarm Profile Editing

Table 10-9 describes the five profile-editing options available when you right-click an alarm item in the profile column (such as Default).

Table 10-9 Alarm Profile Editing Options

Button	Description
Store	Saves a profile in a node or in a file.
Rename	Changes a profile name.
Clone	Creates a new profile that contains the same alarm severity settings as the profile being cloned.
Reset	Restores a profile to its previous state or to the original state (if it has not yet been applied).
Remove	Removes a profile from the table editor.

10.3.4 Alarm Severity Option

To change or assign alarm severity, left-click the alarm severity you want to change in the alarm profile column. Seven severity levels appear for the alarm:

- Not Reported (NR)
- Not Alarmed (NA)
- Minor (MN)
- Major (MJ)
- Critical (CR)
- Use Default
- Transient (T)

Transient and Use Default severity levels only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

10.3.5 Row Display Options

In the network view, the Alarm Profiles window has two check boxes at the bottom of the window:

- Hide values matching profile Default—Highlights alarms with nondefault severities by clearing alarm cells with default severities (disabled in Software Release 5.0).
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

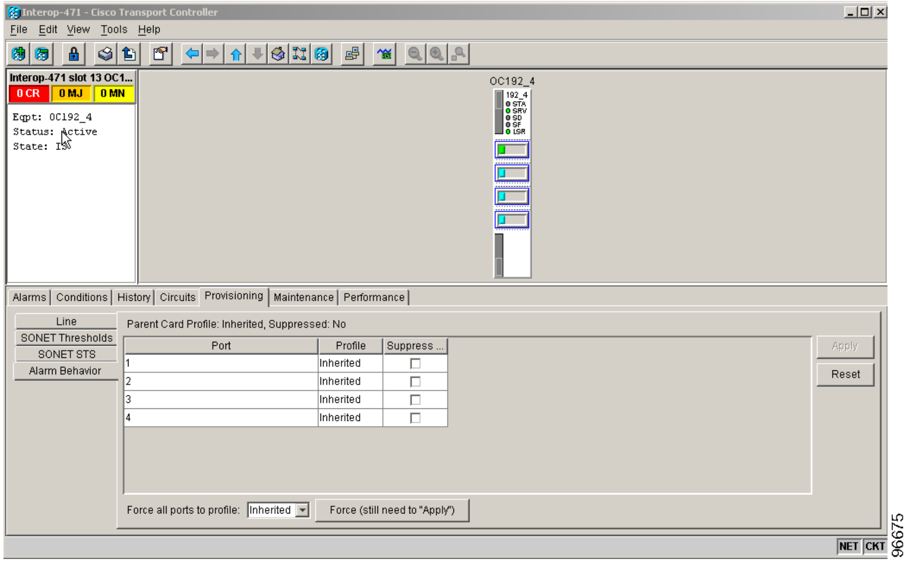
10.3.6 Alarm Profile Applications

In CTC node view, the Alarm Behavior window displays alarm profiles for the node, and in card view the Alarm Behavior window displays the alarm profiles for the selected card.

Alarm profiles form a hierarchy. A node-level alarm profile applies to all cards in the node except cards that have their own profiles. A card-level alarm profile applies to all ports on the card except ports that have their own profiles.

At the node level, you can apply profile changes on a card-by-card basis or set a profile for the entire node. At the card-level view, you can apply profile changes on a port-by-port basis for all ports on that card. Figure 10-7 shows the OC192 LR 1550 card view of an alarm profile.

Figure 10-7 Alarm Profile on the OC192 LR 1550 Card



Eqpt: OC192_4
Status: Active
State: IS

Parent Card Profile: Inherited, Suppressed: No

Port	Profile	Suppress ...
1	Inherited	□
2	Inherited	□
3	Inherited	□
4	Inherited	□

Force all ports to profile: Inherited

10.4 Alarm Filter

Alarm display can be filtered to keep particular alarm severities, or alarms that occur between certain dates, from appearing in the Alarms window (Figure 10-2 on page 10-5). You can set the parameters of the filter by clicking Filter at the bottom-left of the Alarms window. You can turn the filter on or off by clicking the Filter icon button at the bottom-right of the window. CTC retains your filter activation setting. For example, if you turn the filter on and then log out, CTC makes the filter active the next time your user ID is activated.

10.5 Alarm Suppression

The ONS 15600 has suppression options that prevent node, slot, chassis, or port alarms from appearing in the Alarms window. Suppression changes the entity alarm to Not Reported, so suppressed alarms are shown in the Conditions window. The suppressed alarms are shown with their other visual characteristics (service-affecting status and color-coding) in the window. These alarms do not appear in the History window or in any other clients.

In node view, you can suppress all alarms for a node, one or more card slots, fan slots, objects that are not cards such as the chassis, or the customer access panel (CAP). In the card view, you can suppress alarms on a port-by-port basis. All alarms for the entity are suppressed. For example, if you click the Suppress Alarms check box in node view, all node alarms appear in the Conditions window rather than the Alarms window. If you suppress alarms for one or more slots or ports, alarms for those entities appear in the Conditions window.

Note Use alarm suppression with caution. If multiple CTC or TL1 sessions are open, suppressing the alarms in one session suppresses the alarms in all other open sessions.

10.6 External Alarms and Controls

External alarm inputs are used for external sensors such as open doors and flood sensors, temperature sensors, and other environmental conditions. External control outputs allow you to drive external visual or audible devices such as bells and lights. They can control other devices such as generators, heaters, and fans.

You provision external alarms and controls in the node view Provisioning or Maintenance > Alarm Extenders window. Up to 16 external alarm inputs and 16 external controls are available. The external input/output contacts are located on the CAP attached to the ONS 15600 backplane.

10.6.1 External Alarm Input

You can provision each alarm input separately. Provisionable characteristics of external alarm inputs include:

- Alarm type
- Alarm severity (CR, MJ, MN, NA, and NR)
- Alarm-trigger setting (open or closed)
- Virtual wire associated with the alarm
- CTC alarm log description (up to 63 characters)

10.6.2 External Control Output

You can provision each alarm output separately. Provisionable characteristics of alarm outputs include:

- Control type
- Trigger type (alarm or virtual wire)
- Description for CTC
- Closure setting (manually or by trigger). If you provision the output closure to be triggered, the following characteristics can be used as triggers:
  - Local NE alarm severity—A chosen alarm severity (for example, major) and any higher-severity alarm (in this case, critical) causes output closure.
  - Remote NE alarm severity—Similar to local NE alarm severity trigger setting, but applies to remote alarms.
  - Virtual wire entities—You can provision an alarm that is input to a virtual wire to trigger an external control output.

10.6.3 Virtual Wires for External Alarms in Mixed Networks

Virtual wires route external alarms to one or more alarm collection centers in a network. External alarms can be assigned to virtual wires in networks containing only ONS 15600s or in mixed networks containing ONS 15600s, ONS 15454s, and ONS 15327s. You can view virtual wires in the CTC node view Maintenance > Alarm Extenders > Virtual Wires window.

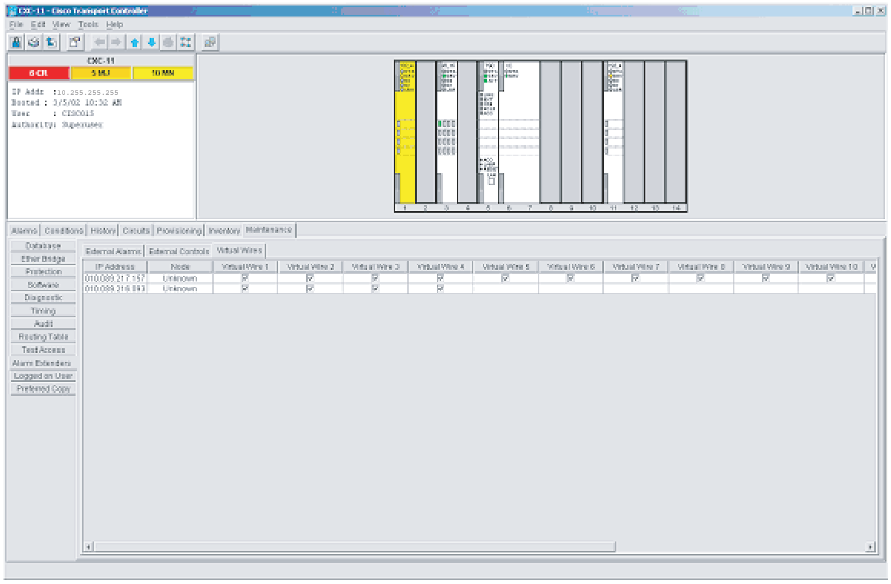
When using virtual wires, you can:

- Assign different external devices to the same virtual wire.
- Assign virtual wires as the trigger type for different external controls.

The ONS 15600 supports 16 virtual wires. The ONS 15454 and ONS 15327 each support four virtual wires. In mixed ONS 15600/15454/15327 networks, CTC displays the virtual wire information differently based upon where it is viewed.

Figure 10-8 shows an ONS 15600 Virtual Wires window with a DCC connection to an ONS 15454 node. The ONS 15600 Virtual Wires window shows 10 virtual wire columns, but 16 are available. The first 12 are available for other ONS 15600s. Only the last four are available for the ONS 15454, because it can only support four virtual wires.

Figure 10-8 Virtual Wires Seen from an ONS 15600

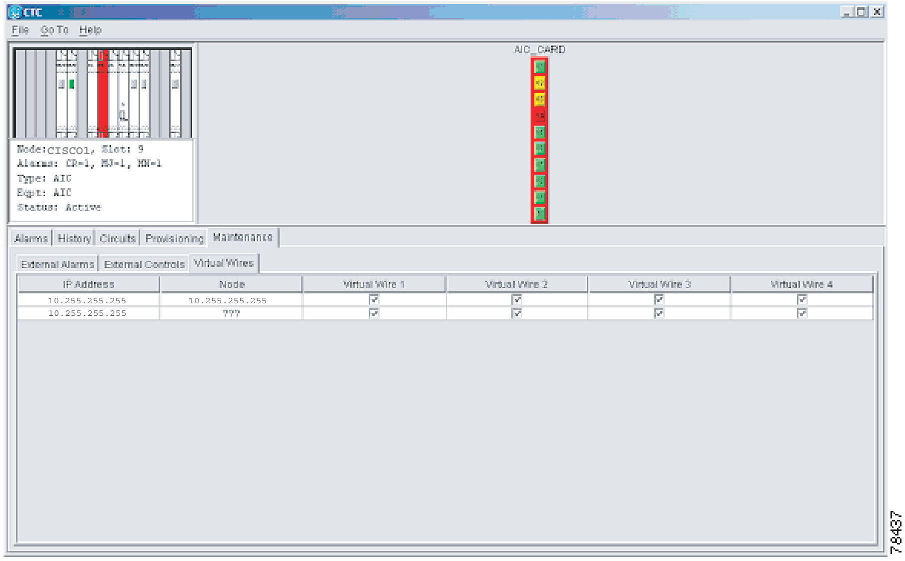


IP Addr : 10.255.255.255
Booted : 3/5/02 10:32 AM
User : CISCO15
Authority: Superuser

IP Address	Node	Virtual Wire 1	Virtual Wire 2	Virtual Wire 3	Virtual Wire 4	Virtual Wire 5	Virtual Wire 6	Virtual Wire 7	Virtual Wire 8	Virtual Wire 9	Virtual Wire 10	V
010.089.217.157	Unknown	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	
010.089.216.093	Unknown	☑	☑	☑	☑							

Figure 10-9 shows the same network configuration as in Figure 10-8, but it appears in the ONS 15454 Virtual Wires window (accessed in the Alarm Interface Controller [AIC] card view Maintenance window). The ONS 15454 shows information for only four virtual wires. Because the ONS 15454 cannot use the top 12 virtual wires, the omission does not affect ONS 15454 usage.

Figure 10-9 Virtual Wires Seen from an ONS 15454



CTC
File Go To Help
AIC_CARD
Alarms History Circuits Provisioning Maintenance
External Alarms External Controls Virtual Wires
78437

Node: CISCO1, Slot: 9
Alarms: CR=1, MJ=1, MN=1
Type: AIC
Eqpt: AIC
Status: Active

IP Address	Node	Virtual Wire 1	Virtual Wire 2	Virtual Wire 3	Virtual Wire 4
10.255.255.255	10.255.255.255	☑	☑	☑	☑
10.255.255.255	???	☑	☑	☑	☑

10.7 Audit Trail

The ONS 15600 maintains an audit trail log that resides on the TSC. This record shows who has accessed the system and what operations were performed during a given period of time and is in accordance with GR-839-CORE. The log includes authorized Cisco logins and logouts using the operating system command line interface, CTC, and TL1; the log also includes FTP actions, circuit creation/deletion, and user/system generated actions.

Event monitoring is also recorded in the audit log. An event is defined as the change in status of an element within the network. External events, internal events, attribute changes, and software upload/download activities are recorded in the audit trail.

Audit trails are useful for maintaining security, recovering lost transactions and enforcing accountability. Accountability is the ability to trace user activities and is done by associating a process or action with a specific user. To view the Audit Trail log, refer to Chapter 7, “Manage Alarms,” in the *Cisco ONS 15600 Procedure Guide*. Users can access the audit trail logs from any management interface (CTC, CTM, TL1).

The audit trail is stored in persistent memory and is not corrupted by processor switches, resets or upgrades. However, if a user pulls both TSCs, the audit trail log is lost.

10.7.1 Audit Trail Log Entries

Audit trail records capture the following activities:

- User—Name of the user performing the action
- Host—Host from where the activity is logged
- Device ID—IP address of the device involved in the activity
- Application—Name of the application involved in the activity

- Task—Name of the task involved in the activity (View a dialog, apply configuration and so on)
- Connection Mode—Telnet, Console, SNMP
- Category—Type of change; Hardware, Software, Configuration
- Status—Status of the user action (Read, Initial, Successful, Timeout, Failed)
- Time—Time of change
- Message Type—Denotes if the event is Success/Failure type
- Message Details—A description of the change

10.7.2 Audit Trail Capacities

The system is able to store 640 log entries.When this limit is reached, the oldest entries are overwritten with new events.

When the log server is 80 percent full, an AUD-LOG-LOW condition is raised and logged (by way of CORBA/CTC).

When the log server reaches a maximum capacity of 640 entries and begins overwriting records that were not archived, an AUD-LOG-LOSS condition is raised and logged. This event indicates that audit trail records have been lost. Until the user off-loads the file, this event occurs once regardless of the amount of entries that are overwritten by the system. To export the Audit Trail log, refer Chapter 7, “Manage Alarms,” in the *Cisco ONS 15600 Procedure Guide*.